

REMARKS

Claims 1-57 and 60-67 are pending. The independent claims are claims 1, 29, 30, 60, 65, and 66. All claims now stand rejected based on new grounds of rejection. Claim 1 is rejected as obvious under 35 U.S.C. § 103(a) from *Hayashi Seiichiro* (JP 09-261218) in view of *Abburi et al.* (USPG PUBs 2003/0084306 A1). Independent claims 29, 30, and 65 are rejected on the same grounds. Independent claims 60 and 66 are rejected as obvious under 35 U.S.C. § 103(a) from *Seiichiro* and *Abburi* in further view of *Lauper et al.* (U.S. Patent No. 7,016,666).

The Present Amendments

The present independent claims are now amended without prejudice, in order to expedite prosecution of the present application. All of the amendments are fully supported by the specification as originally filed, and no new matter is introduced.

The independent claims are amended to specify that the session is a secure socket layer session. The Advisory Action said that “applicant is advised to clearly claim his session.” Therefore, the present claims do so, and this amendment is supported at least by page 13 of the application as originally filed (see line six).

The present independent claims are also now amended to require that the usage limitations furthermore include a limit on use of the key for encryption only, which excludes use of said key for signature verification. This is supported at least by page 13 of the application as originally filed.

Summary of the Present Invention

The present invention includes a method allowing user identification or data encryption with a public key technique, for a user who already has a certificate and corresponding secret key for signatures using another system. For example, a temporary key can be used by allowing the user to create acceptable certificates for those temporary keys. According to other (e.g. prior art) methods, such user-created certificates are not considered valid. In an embodiment of the present invention, user-created certificates are accepted, but they use the identity from a certificate already provided by a certificate authority (CA).

The present application also recognizes and solves a problem related to fraud. The solution of the present claimed invention is to place an appropriate temporal limit on the usage of the certificate. This temporal limit on usage is such that once a session on the other system is completed, then the certificate or a corresponding key is destroyed. The end of a session is the earliest practical point at which to destroy the certificate or key, without disrupting the session, and this insight has led Applicants to the present claimed invention.

The present claimed invention also limits use of said key for encryption only, which excludes use of said key for signature verification. This further limits the potential for fraud, especially in combination with the temporal limit.

The Present Independent Claims Are Not Obvious From The Cited References

Applicant respectfully submits that the present independent claims as amended are not obvious from *Seiichiro* in view of *Abburri*, or in further view of *Lauper*. These references do not disclose a certificate limiting use of the key for encryption only, while excluding use of the key for signature verification, in combination with a temporal limit.

Regarding the temporal limit, present claim 1 discloses that “once a secure socket layer session on the second system is completed, the certificate or a corresponding key is destroyed.” Applicant submits that this session-completion limitation of present claim 1 is different from what is disclosed in the *Abburri* reference. But even if it were the same, still the

cited combination of references does not teach or suggest having the certificate limit use of the key for encryption only, while excluding use of the key for signature verification, as presently claimed.

The final Office Action and the Advisory Action assert that the session-completion limitation of present claim 1 is disclosed by par. 0455, 0463-0469, 0461, and 0452 of *Abburri*. Applicant respectfully submits that this is incorrect, especially in view of the present amendments which clarify that the session is a secure socket layer session.

Paragraph 0455 of *Abburri* only describes destroying a copy/replacement license (i.e. a license for a second system) when the original license expires (i.e. when the license for the first system expires). This is very different from present claim 1, which describes destroying a license for the second system when a session (e.g. a Secure Socket Layer session) on the second system expires.

Likewise, paragraph 0452 of *Abburri* discloses destroying a copy/replacement license for the second system when a fixed time has elapsed (e.g. two days). This fixed time period is completely unrelated to when a session on the second system is completed.

Likewise, paragraph 0461 of *Abburri* discloses destroying a copy/replacement license when thirty (30) days have elapsed since contacting a synchronization server. Again, this fixed time period is completely unrelated to when a session on the second system is completed.

Likewise, paragraphs 0463-0469 merely refers to the expiration schemes already described in *Abburri*, none of which involve expiration when a session ends.

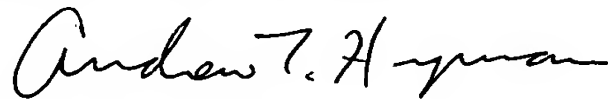
Because *Abburri* nowhere suggests destroying a copy/replacement license once a session on the second system is completed, combining *Abburri* with *Seiichiro* cannot yield the present claimed invention. These same arguments apply to the other independent claims as well. The cited combination of *Abburri* with *Seiichiro* is thus far less effective at combating fraud as compared to the present claimed invention, which utilized the minimum practical amount of time for a copy/replacement license before that license is destroyed.

Application Serial No. 10/090,422
Attorney Docket No. 944-005.002

Conclusion

It is therefore respectfully submitted that the pending claims are now distinguished over the cited art, and that the claims are therefore in condition for allowance. Such action is earnestly solicited.

Respectfully submitted,



Andrew T. Hyman
Attorney for the Applicant
Registration No. 45,858

ATH/mbh
WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, PO Box 224
Monroe CT 06468
(203) 261-1234